Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002514

International filing date: 10 February 2005 (10.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-033355
Filing date: 10 February 2004 (10.02.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2005/002514

10. 2. 2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

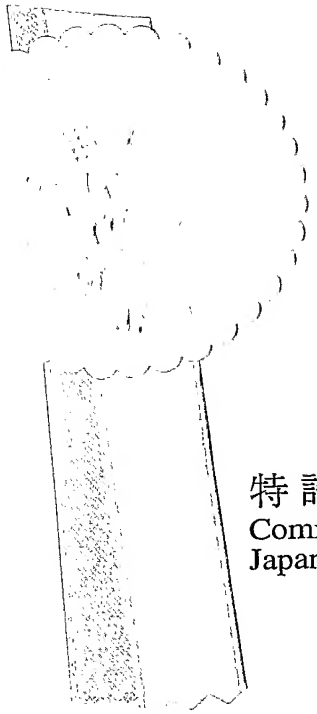
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月１０日

出願番号
Application Number: 特願２００４－０３３３５５

[ST. 10/C]: ［ＪＰ２００４－０３３３５５］

出願人
Applicant(s): エヌ・ティ・ティ・コミュニケーションズ株式会社



２００５年　３月１７日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２３７８５

【書類名】　特許願
【整理番号】　GLN-00470
【提出日】　平成16年 2月10日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　加賀谷　誠
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　荻原　利彦
【発明者】
　【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
　【氏名】　野村　進
【特許出願人】
　【識別番号】　399035766
　【氏名又は名称】　エヌ・ティ・ティ・コミュニケーションズ株式会社
【代理人】
　【識別番号】　100083806
　【弁理士】
　【氏名又は名称】　三好　秀和
　【電話番号】　03-3504-3075
【選任した代理人】
　【識別番号】　100068342
　【弁理士】
　【氏名又は名称】　三好　保男
【選任した代理人】
　【識別番号】　100095500
　【弁理士】
　【氏名又は名称】　伊藤　正和
【選任した代理人】
　【識別番号】　100101247
　【弁理士】
　【氏名又は名称】　高橋　俊一
【選任した代理人】
　【識別番号】　100098327
　【弁理士】
　【氏名又は名称】　高松　俊雄
【手数料の表示】
　【予納台帳番号】　001982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9908855

【書類名】特許請求の範囲
【請求項１】
利用者の機密情報を管理する機密情報管理システムであって、
前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割手段と、
前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶手段と、
必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割手段で作成された分割データとは異なる複数の分割データを生成するデータ再分割手段と、
前記データ再分割手段で作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前記データ再分割手段で作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶手段と、
を有することを特徴とする機密情報管理システム。
【請求項２】
前記機密情報を使用する場合には、前記利用者が保持する分割データを取得し、該分割データと前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする請求項１記載の機密情報管理システム。
【請求項３】
前記機密情報を使用するときには、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする請求項２記載の機密情報管理システム。
【請求項４】
前記機密情報を使用する場合には、前記第２の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする請求項１記載の機密情報管理システム。
【請求項５】
前記第１の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする請求項１乃至４のいずれか１項に記載の機密情報管理システム。
【請求項６】
前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする請求項１乃至５のいずれか１項に記載の機密情報管理システム。
【請求項７】
利用者の機密情報を管理する機密情報管理方法であって、
前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、
前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶ステップと、
必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、
前記データ再分割ステップで作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前

記データ再分割ステップで作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶ステップと、
を有することを特徴とする機密情報管理方法。
【請求項８】
利用者の機密情報を管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、
前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、
前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶ステップと、
必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、
前記データ再分割ステップで作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶ステップと、
前記コンピュータに実行させることを特徴とする機密情報管理プログラム。

【書類名】明細書
【発明の名称】機密情報管理システム、機密情報管理方法、および機密情報管理プログラム
【技術分野】
【０００１】
本発明は、利用者の機密情報を管理する機密情報管理システム、機密情報管理方法、および機密情報管理プログラムに関する。
【背景技術】
【０００２】
ＩＴ（Information Technology）技術の発展に伴って、パスワード、クレジット番号などが入った携帯電話および携帯情報端末、並びにＰＫＩ秘密鍵が入ったＩＣカードなどを用いて、所望のサービスの提供を受ける機会が増えている。例えば、ユーザのパスワードを使用してログインし、情報を閲覧したり、ユーザのクレジットカード番号を使用して物品購入したりするようなサービスが普及している。
【０００３】
このような機会において、ユーザが上述した機密情報（例えば、パスワード、クレジット番号およびＰＫＩ秘密鍵など）が記憶されている携帯電話、携帯情報端末およびＩＣカードなどを紛失した場合には、紛失した旨を発行元に申告して、該機密情報を失効させ、新たに機密情報を再発行してもらう必要がある。
【非特許文献１】電子認証システム推進検討会、“企業間電子商取引システムにおける電子認証システムの仕様に関するガイドライン”、[Online]、[平成１６年１月２０日検索]、インターネット＜ＵＲＬ：http://www.ecom.or.jp/home/g12.pdf＞
【発明の開示】
【発明が解決しようとする課題】
【０００４】
そのため、ユーザが保持する機密情報を紛失した際には、セキュリティ維持のため、紛失した機密情報を失効させるとともに、機密情報を変更しなければならないという課題がある。また、機密情報を変更するため、再発行まではサービスの提供を受けることができないという課題もある。
【０００５】
本発明は、上記の課題を解決するためになされたものであり、ユーザが保持する携帯電話、携帯情報端末、ＩＣカードなどを紛失しても、機密情報を変更することなくサービスの提供を受けることが可能な機密情報管理システム、機密情報管理方法、および機密情報管理プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記目的を達成するため、請求項１記載の本発明は、利用者の機密情報を管理する機密情報管理システムであって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割手段と、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶手段と、必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割手段で作成された分割データとは異なる複数の分割データを生成するデータ再分割手段と、前記データ再分割手段で作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前記データ再分割手段で作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶手段と、を有することを特徴とする。
【０００７】
請求項２記載の本発明は、請求項１記載の発明において、前記機密情報を使用する場合

には、前記利用者が保持する分割データを取得し、該分割データと前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段を有することを特徴とする。

【０００８】

請求項３記載の本発明は、請求項２記載の発明において、前記機密情報を使用するときには、使用した事実を使用履歴情報として記憶する使用履歴記憶手段を有することを特徴とする。

【０００９】

請求項４記載の本発明は、請求項１記載の発明において、前記機密情報を使用する場合には、前記第２の記憶部に記憶された各分割データのうち、前記所定の個数から前記利用者が保持する分割データの個数を引いた個数の分割データの組み合わせを前記利用者が有する端末に通信ネットワークを介して送信する分割データ送信手段を有することを特徴とする。

【００１０】

請求項５記載の本発明は、請求項１乃至４のいずれか１項に記載の発明において、前記第１の記憶部に記憶される分割データを通信ネットワークを介して前記利用者が有する端末に送信する送信手段を有することを特徴とする。

【００１１】

請求項６記載の本発明は、請求項１乃至５のいずれか１項に記載の発明において、前記機密情報を前記利用者が有する端末から通信ネットワークを介して受信する受信手段を有することを特徴とする。

【００１２】

請求項７記載の本発明は、利用者の機密情報を管理する機密情報管理方法であって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、前記データ再分割ステップで作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶ステップと、を有することを特徴とする。

【００１３】

請求項８記載の本発明は、利用者の機密情報を管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、前記機密情報を秘密分散法を用いて、該機密情報が所定の個数から復元できる複数の分割データに分割するデータ分割ステップと、前記複数の分割データの一部を、前記利用者が保持するための分割データとして第１の記憶部に記憶させるとともに、前記複数の分割データの残りを、１又は複数の第２の記憶部それぞれに記憶させるデータ記憶ステップと、必要に応じて前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データのうち前記所定の個数の分割データの組み合わせから前記機密情報を前記データ分割ステップで作成された分割データとは異なる複数の分割データを生成するデータ再分割ステップと、前記データ再分割ステップで作成された前記複数の分割データの一部を前記第１の記憶部に記憶させるとともに、前記第２の記憶部に記憶された各分割データを無効にして、前記データ再分割ステップで作成された前記複数のデータの残りを前記第２の記憶部それぞれに記憶させるデータ再記憶ステップと、前記コンピュータに実行させることを特徴とする。

【発明の効果】

【００１４】

本発明に係わる機密情報管理システム、機密情報管理方法、および機密情報管理プログラムによれば、機密情報を秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割情報の紛失があったとしても、残りの分割情報から機密情報を復元できるとともに、秘密分散法を用いて新たに機密情報を再分割し、該再分割情報の一部を新たにユーザに保持させるので、機密情報の変更は不要である。

【００１５】

この結果、ユーザが保持する分割情報の紛失があったとしても、機密情報の再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の実施の形態を図面を用いて説明する。

【００１７】

図１は、本発明の実施の形態に係る機密情報管理システム１が適用されるコンピュータシステム１０全体の概略構成を示すブロック図である。

【００１８】

図１に示すように、機密情報管理システム１は、インターネット等の通信ネットワーク４を介してユーザが備えるクライアント端末（以下、単に端末とよぶ）２と接続されているとともに、通信ネットワーク４を介して所定のサービスを提供するサービス提供システム５と接続されている。また、機密情報管理システム１は、ハードウェア的に互いに独立した複数（本実施の形態では３とする）のデータ保管用サーバコンピュータ（以下、単に保管サーバとよぶ）３ａ，３ｂ，３ｃと接続されている。

【００１９】

尚、本実施の形態における機密情報とは、ユーザがサービス提供システム５を利用するために必要なパスワード、クレジットカード番号、ＰＫＩ秘密鍵などの個人情報をいう。

【００２０】

上記構成のコンピュータシステム１０においては、端末２が所定のサービスをサービス提供システム５から受ける際に必要とされる機密情報Ｓを機密情報管理システム１に送信すると、機密情報管理システム１において秘密分散法を用いて該機密情報Ｓを複数のデータに分割し、該分割データを保管サーバ３ａ，３ｂ，３ｃおよび端末２にそれぞれ送信し、保管させるようになっている。この結果、機密情報Ｓが機密情報管理システム１に登録されたことになり、ユーザはサービス利用の準備が整ったことになる。尚、図１では、機密情報管理システム１は、端末２からの機密情報Ｓを４つの分割データD(1)，D(2),D(3),D(4)に分割し、それぞれを複数の保管サーバ３ａ，３ｂ，３ｃおよび端末２に保管するようになっている。

【００２１】

また、サービス利用時は、端末２から機密情報管理システム１に対して、ユーザが保持する分割データD(4)を送信すると、機密情報管理システム１は、該分割データD(4)および保管サーバ３ａ，３ｂ，３ｃの分割データD(1),D(2),D(3)の所定の組み合わせから秘密分散法を用いてもとの機密情報Ｓを復元し、該機密情報Ｓをサービス提供システム５に送信するようになっている。これにより、機密情報Ｓの正当性が確認されれば、ユーザは所定のサービスの提供を受けることができる。

【００２２】

機密情報管理システム１は、詳しくは、機密情報Ｓから秘密分散法を用いて複数の分割データＤに分割する分割データ生成部１１、複数の分割データＤから元データ（機密情報）Ｓを復元する元データ復元部１２、機密情報システム１がサービス提供システム５に機密情報Ｓを送信した事実をサービス使用履歴として生成する使用履歴生成部１３、および端末２、保管サーバ３ａ，３ｂ，３ｃおよびサービス提供システム５それぞれとデータの送受信を行う通信部１４を具備する構成となっている。

【００２３】

また、端末２は、ユーザが携行可能な携帯情報端末、携帯電話、ＩＣカードなどの携帯

記憶媒体などが想定されるが、他にモバイルを用途としないコンピュータ機器であってもよいものである。

【００２４】

ここで、上述した機密情報管理システム１、端末２、保管サーバ３ａ，３ｂ，３ｃおよびサービス提供システム５は、それぞれ少なくとも演算機能および制御機能を備えた中央演算装置（ＣＰＵ）、プログラムやデータを格納する機能を有するＲＡＭ等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置およびシステムは、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。

【００２５】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【００２６】

次に、本実施の形態に係る機密情報管理システム１が適用されるコンピュータシステム１０全体の動作について説明する。ここで、図２は、ユーザが機密情報Ｓを機密情報管理システム１に登録する動作を説明するシーケンス図であり、図３は、ユーザがサービスを利用する時の機密情報管理システム１の動作を説明するシーケンス図であり、図４は、ユーザが保持する分割データＤを紛失したときの機密情報管理システム１の動作を説明するシーケンス図である。

【００２７】

（１）　機密情報登録処理

まず、ユーザが端末２から通信ネットワーク４を介して機密情報管理システム１に機密情報Ｓを送信する（ステップＳ１０）。機密情報管理システム１は、機密情報Ｓを受け取ると、秘密分散法を用いて４つのデータ（分割データ）D(1),D(2),D(3),D(4)に分割する（ステップＳ２０）。

【００２８】

ここで、ステップＳ２０の秘密分散法に基づく分割データ生成処理について詳細に説明する。

【００２９】

例えば、２次多項式Ｆ（ｘ）＝ａｘ^2＋ｂｘ＋Ｓ（ｍｏｄ　ｐ；ｐで割った時の余りを表す）を基にしたＳｈａｍｉｒの秘密分散法｛（ｋ、ｎ）閾値法；但し、分割数を表すｎを４とし、復元できる数を表すｋを３とする｝で考える。ここでＳは元データである機密情報、Ｆ（ｘ）は分割データである。ａ、ｂ、ｐは、機密情報Ｓの分割に際して任意に決定される。但し、ｐは、ａ、ｂ、Ｓよりも大きい素数とする。

【００３０】

このとき、機密情報管理システム１の分割データ生成処理により、分割データF(1)，F(2),F(3),F(4)｛上記分割データD(1),D(2),D(3),D(4)に対応｝は、次式（１）～（４）のように作成される。

【００３１】

Ｆ（１）＝ａ＋ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（１）

Ｆ（２）＝４ａ＋２ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（２）

Ｆ（３）＝９ａ＋３ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（３）

Ｆ（４）＝１６ａ＋４ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（４）

この分割データF(1)，F(2),F(3),F(4)の内、ｋ＝３以上の分割データ｛例えば、F(1),F(2),F(4)｝が集まれば、この分割データ

Ｆ（１）＝ａ＋ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（１）

Ｆ（２）＝４ａ＋２ｂ＋Ｓ（ｍｏｄ　ｐ）　　・・・（２）

Ｆ（４）＝１６ａ＋４ｂ＋Ｓ（ｍｏｄ　ｐ）　・・・（４）
を連立して元データＳを求めることができる。そして、ｋ－１以下の分割データが集まっても、元データＳを復元することはできない。

【００３２】

次に、機密情報管理システム１は、このようにして生成された分割データを各保管サーバ３ａ，３ｂ，３ｃおよび端末２にネットワーク４を介して送信する（ステップＳ３０）。

【００３３】

次に、保管サーバ３ａ，３ｂ，３ｃは、それぞれ送信されてきた分割データD(1),D(2),D(3)をハードディスク等の記憶装置に記憶する（ステップＳ４０）。また、端末２は、送信されてきた分割データD(4)をハードディスク等の記憶装置に記憶する（ステップＳ５０）。

【００３４】

これにより、端末２、保管サーバ３ａ，３ｂ，３ｃのうちいずれか１つの分割データに紛失、破壊等があっても、残りの３つの分割データからもとの機密情報Ｓを復元できる（Ｓｈａｍｉｒの秘密分散法において分割数を４とし、復元できる数を３とする場合）。

【００３５】

（２）サービス利用処理

ユーザがサービス提供システム５を利用する場合には、まず、端末２に保持する分割データD(4)を通信ネットワークを介して機密情報管理システム１に送信する（ステップＳ１１０）。

【００３６】

機密情報管理システム１は、端末２から分割データD(4)を受け取ると、残りの分割データD(1)，D(2)を保管サーバ３に要求し（Ｓｈａｍｉｒの秘密分散法にて分割数を４とし、復元できる数を３とする場合）、該分割データD(1)，D(2)を受け取る（ステップＳ１２０）。尚、この場合には、３つの分割データは任意の組み合わせでよく、例えば、上述したようにD(1)，D(2)，D(4)の組み合わせの他、D(1)，D(2)，D(3)の組み合わせ、D(1)，D(3)，D(4)の組み合わせ、D(2)，D(3)，D(4) の組み合わせのいずれでもよい。

【００３７】

次に、機密情報管理システム１は、分割データD(1)，D(2),D(4)から秘密分散法を用いて機密情報Ｓを復元する（ステップＳ１３０）。そして、復元した機密情報Ｓをサービス提供システム５に送信して（ステップＳ１４０）、機密情報Ｓを復元し送信した事実を使用履歴として生成する（ステップＳ１５０）。

【００３８】

サービス提供システム５は、機密情報管理システム１から機密情報Ｓを受け取ると、該機密情報Ｓの正当性を判断して、端末２に通信ネットワーク４を介してサービス提供を行う（ステップＳ１６０，Ｓ１７０）。これにより、ユーザは所望のサービスの提供を受けることができる。

【００３９】

（３）分割データ紛失時処理

ユーザが分割データD(4)を紛失した場合（例えば、分割データD(4)を記憶している端末２を紛失した場合）には、まず、機密情報管理システム１にその旨を申告する（例えば、機密情報管理システム１の運用者へ電話連絡する）（ステップＳ２１０）。

【００４０】

これにより、機密情報システム１は、保管サーバ３ａ，３ｂ，３ｃに分割データを要求し、保管サーバ３ａ，３ｂ，３ｃからそれぞれ分割データD(1)，D(2),D(3)を受け取る（Ｓｈａｍｉｒの秘密分散法にて分割数を４とし、復元できる数を３とする場合）（ステップＳ２２０）。

【００４１】

次に、機密情報管理システム１は、分割データD(1),D(2),D(3)から秘密分散法を用いて

機密情報Ｓを復元する（ステップＳ２３０）。そして、復元した機密情報Ｓを、再び秘密分散法を用いて新たに４つのデータ（分割データ）D'(1),D'(2),D'(3),D'(4)に分割する（ステップＳ２４０）。

【００４２】

ここで、分割データD'(1),D'(2),D'(3),D'(4)は、それぞれ最初に生成された分割データD(1),D(2),D(3),D(4)とは異なるデータで、具体的には、上述した２次多項式Ｆ（ｘ）＝ａｘ^{2}＋ｂｘ＋Ｓにおいて、最初の分割時におけるａおよびｂとは異なるａ'およびｂ'を用いて生成された分割データである。

【００４３】

次に、機密情報管理システム１は、このようにして生成された再分割データを各保管サーバ３ａ，３ｂ，３ｃおよび端末２（例えば、ユーザが分割データD(4)を記憶している端末２を紛失した場合には、ユーザが新たに購入した端末２）にネットワーク４を介して送信する（ステップＳ２５０）。

【００４４】

次に、保管サーバ３ａ，３ｂ，３ｃは、それぞれ送信されてきた再分割データD'(1),D'(2),D'(3)をハードディスク等の記憶装置に記憶する（ステップＳ２６０）。また、端末２は、送信されてきた分割データD'(4)をハードディスク等の記憶装置に記憶する（ステップＳ２７０）。これにより、ユーザは再びサービス利用が可能となる。

【００４５】

従って、本実施の形態によれば、所定のサービスを受ける際に必要とされる機密情報Ｓを秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報を復元できるとともに、秘密分散法を用いて新たに機密情報を再分割し、該再分割データの一部を新たにユーザに保持させるので、機密情報Ｓの変更は不要である。

【００４６】

この結果、ユーザが保持する分割データの紛失があったとしても、機密情報Ｓの再発行処理をすることなく、紛失の申告をするだけで、再びサービス提供を受けることができる。

【００４７】

また、紛失した分割データを取得した第３者が機密情報管理システム１にアクセスしても機密情報Ｓを復元することができないので、サービスを利用することができず、安全性が確保される。

【００４８】

さらに、ユーザの使用履歴が機密情報管理システム１に保管されるので、ユーザが分割データを紛失してから紛失した旨を申告するまでの間に、仮に第３者が分割データを取得してサービスを悪用したとしても、使用履歴により悪用の有無を判別することができる。

【００４９】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、端末２から機密情報Ｓの機密情報管理システム１への受け渡しを通信ネットワーク４を介して行ったが、本発明はこれに限定されず、例えば、機密情報Ｓを記録した記録媒体を郵送など通信ネットワーク３以外の手段を介して受け渡してもよい。また、同様に、ユーザが保持する分割データも通信ネットワーク４を介して受け取ったが、本発明はこれに限定されず、例えば、分割データを記録した記録媒体を郵送など通信ネットワーク３以外の手段を介して受け取ってもよい。

【００５０】

また、上記実施の形態よれば、秘密分散法としてＳｈａｍｉｒの秘密分散法｛（ｋ、ｎ）閾値法；但し、分割数を表すｎを４とし、復元できる数を表すｋを３とする｝を用いたが、本発明はこの構成に限定されるものではなく、上記実施の形態で述べた分割数以外の他の分割数、および上記実施の形態で述べた秘密分散法以外の他の秘密分散法を用いるこ

とも可能である。

【００５１】

また、上記実施の形態においては、ユーザがサービス利用時には、機密情報管理システム１が機密情報を復元したが、本発明はこれに限定されず、ユーザの端末２が、端末２に記憶される分割データと機密情報管理システム１から取得した分割データから、秘密分散法を用いて機密情報を復元し、該機密情報をサービス提供システム５に送信してもよいものである。尚、この場合には、復元された機密情報が端末２に記憶されたままユーザが端末２を紛失すると、本発明が解決しようとする課題が解決できないことになるため、該機密情報をサービス提供システム５に送信後すぐに端末２から消去する仕組み、あるいは、端末２のデータの第三者による不正な取り出しを防止する仕組みなどを備えることが必要である。

【００５２】

さらに、上記実施の形態においては、ユーザからの要求により再分割処理を行ったが、機密情報管理システム１が自発的に所定の契機により再分割処理を行ってもよいものである。

【図面の簡単な説明】

【００５３】

【図１】本発明の実施の形態に係る機密情報管理システムが適用されるコンピュータシステム全体の概略構成を示すブロック図である。

【図２】本発明の実施の形態に係る機密情報管理システムにおいて機密情報を登録する処理を説明するシーケンス図である。

【図３】本発明の実施の形態に係る機密情報管理システムにおいてサービス利用時の処理を説明するシーケンス図である。

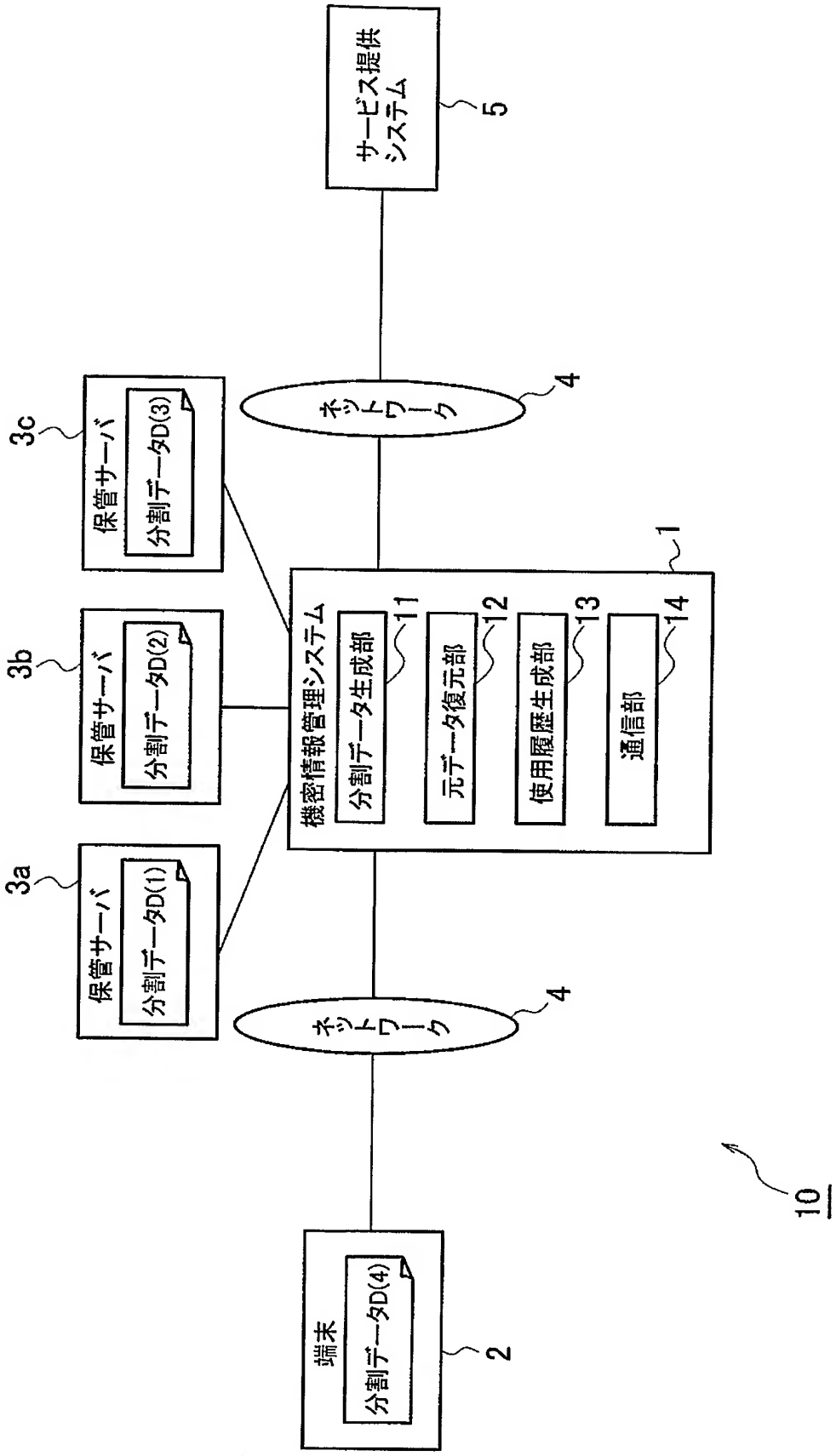
【図４】本発明の実施の形態に係る機密情報管理システムにおいてユーザが保持する機密情報の一部を紛失したときの処理を説明するシーケンス図である。

【符号の説明】

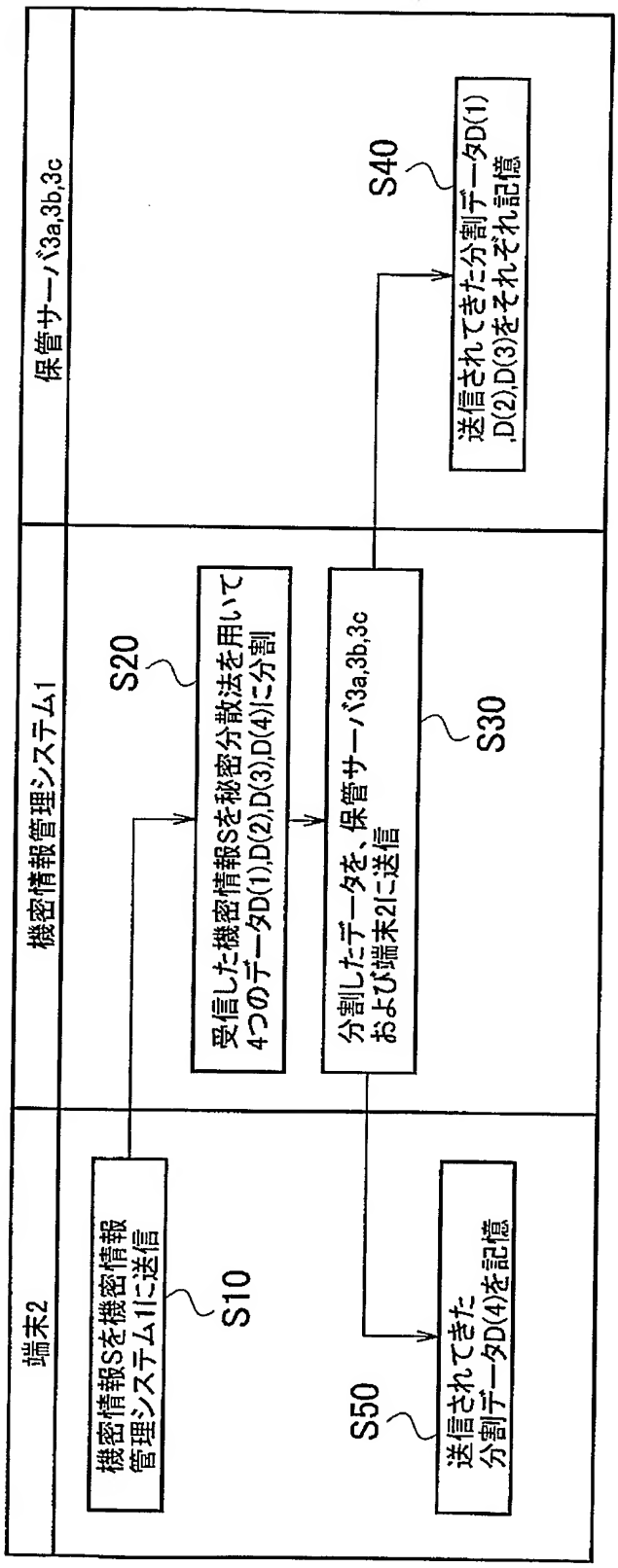
【００５４】

１…機密情報管理システム
２…端末
３ａ，３ｂ，３ｃ…保管サーバ
４…通信ネットワーク
５…サービス提供システム
１０…コンピュータシステム
１１…分割データ生成部
１３…元データ復元部
１５…使用履歴生成部
１７…通信部

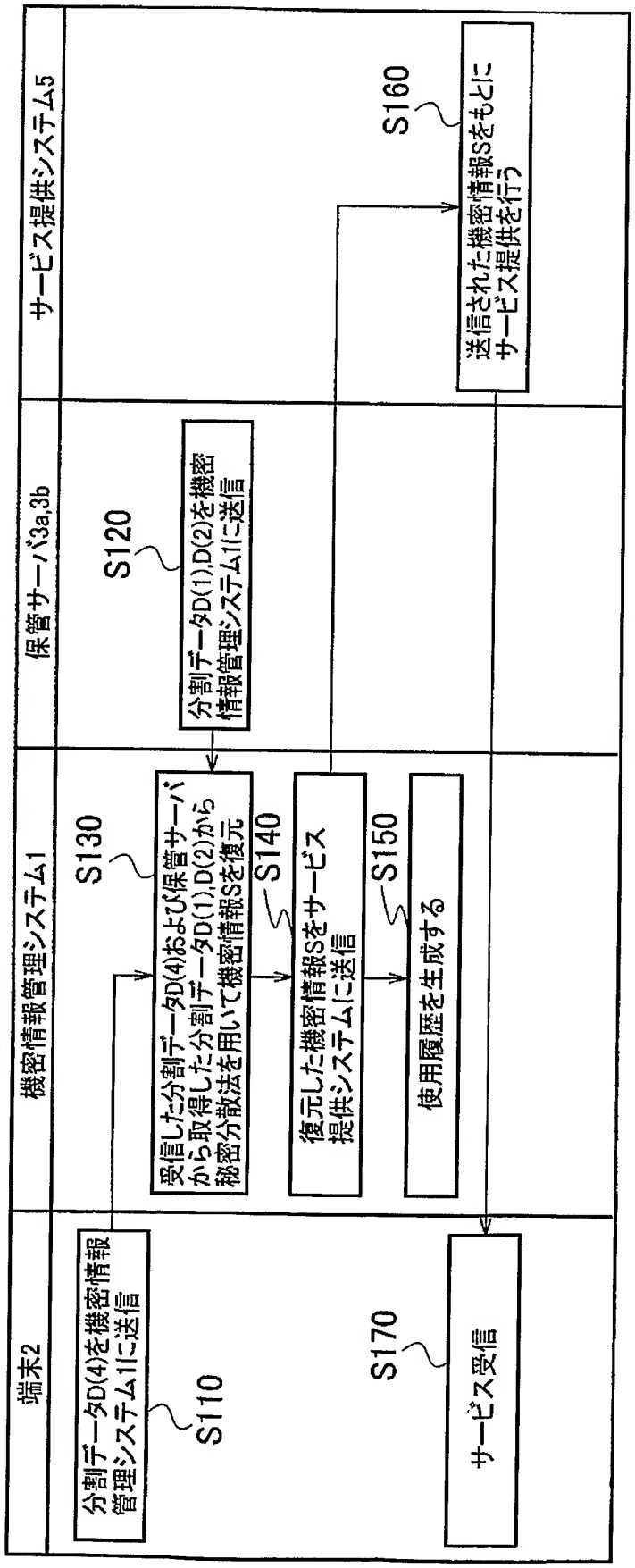
【書類名】図面
【図１】


サービス提供システム
5
ネットワーク
4
保管サーバ
分割データD(3)
3c
保管サーバ
分割データD(2)
3b
保管サーバ
分割データD(1)
3a
機密情報管理システム
1
分割データ生成部
11
元データ復元部
12
使用履歴生成部
13
通信部
14
ネットワーク
4
端末
分割データD(4)
2
10

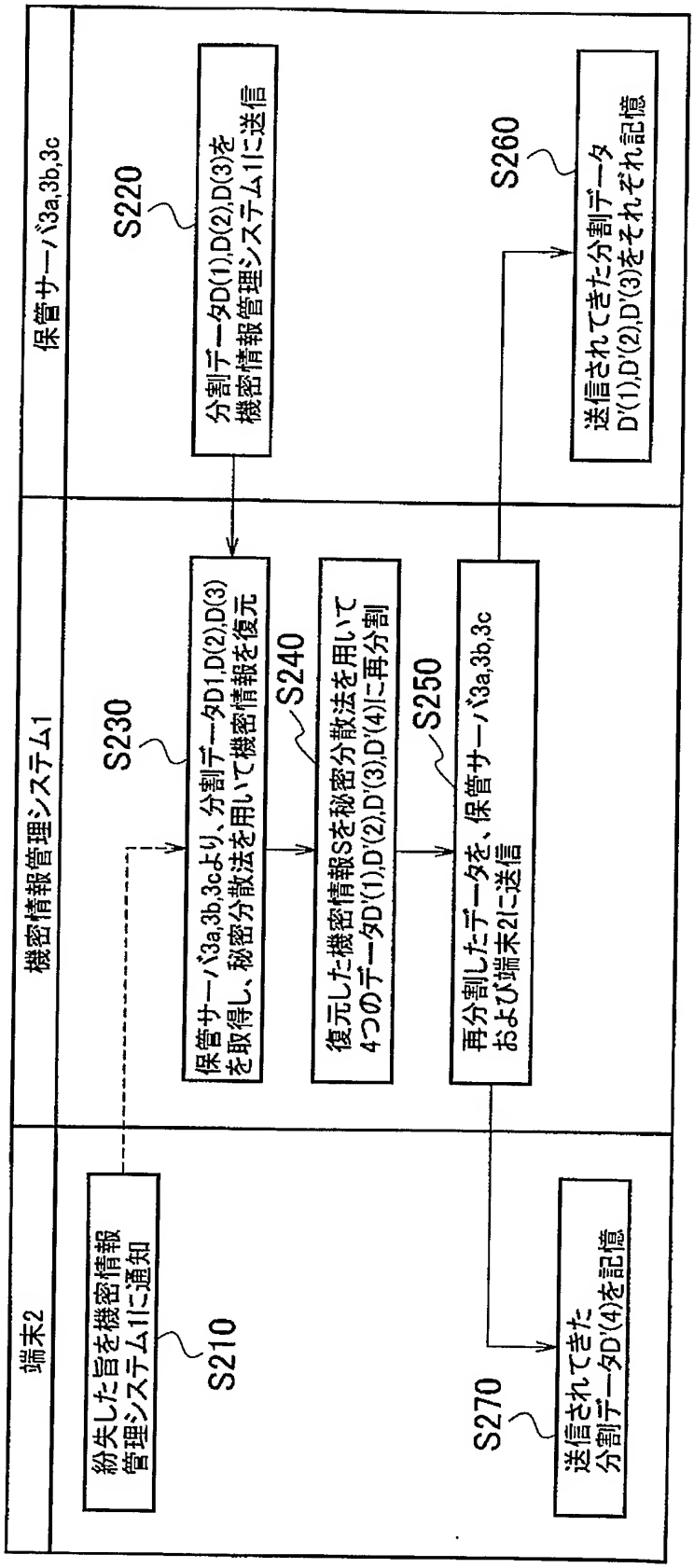
【図２】


端末2
機密情報管理システム1
保管サーバ3a,3b,3c
機密情報Sを機密情報管理システム1に送信
S10
受信した機密情報Sを秘密分散法を用いて4つのデータD(1),D(2),D(3),D(4)に分割
S20
分割したデータを、保管サーバ3a,3b,3cおよび端末2に送信
S30
送信されてきた分割データD(4)を記憶
S50
送信されてきた分割データD(1),D(2),D(3)をそれぞれ記憶
S40

【図３】


端末2
機密情報管理システム1
保管サーバ3a,3b
サービス提供システム5
分割データD(4)を機密情報管理システム1に送信
S110
S120
分割データD(1),D(2)を機密情報管理システム1に送信
S130
受信した分割データD(4)および保管サーバから取得した分割データD(1),D(2)から秘密分散法を用いて機密情報Sを復元
S140
復元した機密情報Sをサービス提供システムに送信
S150
使用履歴を生成する
S160
送信された機密情報Sをもとにサービス提供を行う
S170
サービス受信

【図４】


端末2
機密情報管理システム1
保管サーバ3a,3b,3c
紛失した旨を機密情報管理システム1に通知
S210
保管サーバ3a,3b,3cより、分割データD1,D(2),D(3)を取得し、秘密分散法を用いて機密情報を復元
S230
分割データD(1),D(2),D(3)を機密情報管理システム1に送信
S220
復元した機密情報Sを秘密分散法を用いて4つのデータD'(1),D'(2),D'(3),D'(4)に再分割
S240
再分割したデータを、保管サーバ3a,3b,3cおよび端末2に送信
S250
送信されてきた分割データD'(4)を記憶
S270
送信されてきた分割データD'(1),D'(2),D'(3)をそれぞれ記憶
S260

【書類名】要約書
【要約】
【課題】　ユーザが保持するサービス利用のための情報を紛失しても、機密情報を変更することなくサービスの提供を受けることができる。
【解決手段】　端末２が機密情報Ｓを機密情報管理システム１に送信すると、機密情報管理システム１は秘密分散法を用いて機密情報Ｓを複数のデータに分割し、分割データを保管サーバ３ａ，３ｂ，３ｃ及び端末２に保管させる。サービス利用時は、端末２から分割データを機密情報管理システム１に送信すると、機密情報管理システム１は、該分割データおよび保管サーバの分割データから秘密分散法を用いて機密情報Ｓを復元し、機密情報Ｓをサービス提供システム５に送信する。ユーザが分割データを紛失した際は、機密情報管理システム１は、保管サーバ３ａ，３ｂ，３ｃの分割データから秘密分散法を用いて機密情報Ｓを復元し、機密情報Ｓを再分割して、該再分割データを保管サーバ３ａ，３ｂ，３ｃ及び端末２に保管させる。
【選択図】　図１

特願２００４－０３３３５５

出願人履歴情報

識別番号　［３９９０３５７６６］

１．変更年月日　１９９９年　６月　９日
［変更理由］　新規登録
住　所　東京都千代田区内幸町一丁目１番６号
氏　名　エヌ・ティ・ティ・コミュニケーションズ株式会社